Cooley

October 22, 2015

It's been over two weeks since the European Court of Justice (CJEU) sent shock waves through the almost 4,500 companies that had previously relied on the US-EU Safe Harbor framework. Read more about the ruling. These companies can no longer rely on the framework for safe passage of personal data from the EEA to the United States and, while there is not necessarily a need for mass panic, they must now try to find alternative adequate routes before 31 January 2016.

Article 29 Working Party

The Article 29 Working Party (The Working Party), a European advisory group made up of data protection officials from across Europe, met on Thursday 15th October to discuss the consequences and next steps following the CJEU ruling and released a statement the following day.

The main message was that EU data protection authorities (DPAs) are taking this seriously and that they believe it is absolutely essential to have a robust, collective and common position on the implementation of the judgment. Collaboration is also key and they "urgently called" on Member States and European institutions to open discussions with US authorities to find political, legal and technical solutions that respect EU citizens' fundamental rights. Whilst the Working Party finds data transfer via Safe Harbor unlawful, it still considers alternative methods such as Standard Contractual (or "Model") Clauses and Binding Corporate Rules lawful, but these will now be more closely analysed in light of the judgment. Companies have, however, been given a grace period until the end of January 2016 to implement appropriate alternative methods of transferring personal data to the US, after which time, EU data protection authorities will be committed to taking all necessary and appropriate actions, which may include coordinated enforcement actions.

Global impact

Amongst the aftermath of the ruling, there remains a rather large elephant in the room, which is the future of global surveillance. Following the Snowden revelations, multiple countries have been criticised for finding loop holes in international privacy laws in a "bazaar" of data collection as Snowden called it, where intelligence services in Europe swap collected information and data.

It is important to remember that this decision is not only an EU or even a transatlantic problem. This week, Israel's data protection authority (the Israeli Law Information and Technology Authority, or, ILIT) also stated that multinational companies can no longer rely on Safe Harbor for transferring data to the US. ILIT plans to further investigate the implications and will provide any further findings or clarifications as necessary. Many more countries may follow Israel's lead and we should not rule out the possibility that the European Commission will reconsider whether countries it previously considered as providing "adequate" protection to personal data, actually still do.

What say the USA?

The US Department of Commerce is open for business and, according to its website, is still accepting Safe Harbor applications, which is perhaps a little hopeful.

As pointed out by the European Commissioner for Justice, Consumers and Gender Equality, the negotiations on "Safe Harbor 2" and the umbrella agreement continue, and there is undoubtedly added pressure on these negotiations following the invalidation of the European Commission's Safe Harbor Decision.

Back to the future

As to what the future holds, this is difficult to foretell. If the billion dollar companies are seamlessly implementing

alternative ways of getting personal data to the US, what has really changed in terms of surveillance? The US will need to do its best to negotiate a new, better Safe Harbor, but there are concerns as to whether this is even possible: in a post 9-11 world, will the US and other government agencies around the world ever give up their rights to circumvent privacy laws?

For now, you are safe with Model Clauses, BCRs and other approved mechanisms of cross-border data transfer, but these safety nets could be short-lived once the Working Party put them under their microscope. Last week, Germany's Schleswig-Holstein authority stated that on strict interpretation of the CJEU ruling, transfers on the basis of Model Clauses should no longer be permitted and that consent may not be a valid alternative as informed consent requires a notification of the risks of processing and an informed choice to waive comparable or adequate protections. This decision is restricted to Germany and it remains to be seen whether the views expressed regarding consent will be any more than just thoughts on this subject area. For now, consent remains a valid mechanism for data transfer out of the EEA and we do not believe the DPAs will be quick to remove this as an option for international data transfer.

For businesses previously relying on Safe Harbor there is a risk assessment to be made. How much will it cost you to implement alternatives? The fines may not seem so scary now, but when the General Data Protection Regulation comes into play they will increase to up to €1 million, or between 2% to 5% of gross annual turnover. Increased litigation and claims from individuals may also be on the horizon. Different industries have different options; we can help deal with the consequences and risks in the aftermath of the ruling. Please see our sector-specific advice or contact Sarah Pearce.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.